REMARKS

Claims 1-21 are in the application.

Claims 1-21 are finally rejected as being anticipated under 35 U.S.C. § 102(e) over Winneg et al., US 7,069,586.

Claim 1 provides a secure user interface method, for interacting with a user through a browser, comprising: controlling the browser to request a document from a cooperative server, the browser providing data export support functionality; receiving data with the browser in response to the request; automatically determining, based on a type encoding of the received data, whether a secure browser or a normal browser is to be employed, the secure browser having a set of functionality restricted with respect to the normal browser, to enhance security of a received document against data export; receiving the secure content for presentation in the secure browser; and communicating an input from the user, through the secure browser, to a cooperative server.

It is especially noted that the decision of whether to employ a secure browser or a normal browser is automatically determined based on a type of encoding of the received data. Therefore, in accordance with claims 1-8, it is not the server, but the client, which automatically determines which browser to employ, and that this determination is automatically made based on a type encoding of the received data.

On the other hand, Winneg et al. appears to provide a system in which a local software application controls the client computer independent of a type encoding of the received data. For example, Col. 6, lines 35-48 describe a system which defaults to a "secure" mode, and is machine status dependent, not received data dependent. Indeed, the authorization to access or delete an exam is provided within the "secure" mode, and thus these functions are all provided within a single "browser" or its analog. Therefore, the decisions 114, 116 do not serve to switch "browsers". Col. 8, lines 48- Col. 9, line 44. Therefore, throughout the entire exam process, the machine is locked in a "secure" mode, maintaining this mode apparently independent of received data.

Col. 9, lines 59-67 provide that it is the information entered in the fields of Fig. 7 that are used to determine if content is to be displayed by "the first application" (e.g., MS Word). Fig. 7 shows a login screen, in which a user enters class name, professor and exam date. This does not correspond to the document requested by the browser from the cooperative server, and received by the browser in response to the request, as provided by claim 1.

Therefore, it is seen that Winneg et al. employ a presumption that so long as the exam-taking application is engaged, the machine must be in the "secure" mode, and do not employ encoding of requested data received from the server to automatically control the functionality of a browser. This differs from the present invention in accordance with claim 1, which permits, for example, the server to dynamically control the browser based on data encoding.

Claim 9 provides a secure user interface method, for interacting with a user through a browser, the browser providing a set of navigational functionality, comprising: requesting a document from a cooperative server; receiving data in response to the request; automatically determining whether a secure browser is required to be employed by a content provider or whether an insecure browser is to be employed, the secure browser restricting interaction of the user with tasks other than those permitted by the secure browser which are permitted by the insecure browser; invoking the secure browser; receiving the secure content for presentation in the secure browser; and communicating an input from the user, through the secure browser, to a cooperative server.

This claim therefore provides that the decision of whether a secure browser is required to be employed is automatically determined by a content provider of the secure content, received from the cooperative server. While the elements of claim 9 have some differences from claim 1, the same distinctions as discussed above therefore also apply to claims 9-21.

The various dependent claims are therefore distinguished at least based on the distinctions of the independent claims. However, special mention is made that applicants respectfully traverse the rejection of claims 12 and 19. Fig. 8 and accompanying text do not appear to describe any communications with a remoter server for the purpose of authenticating the "secure browser" or its analog. It appears that Winneg et al. provide a self-authentication process of the secure application at the user's machine. See, e.g., Col. 21, lines 17-27. Likewise, the login procedure described in Col. 8, lines 29-47 appears to be dependent on an authentication of the user-entered data, and not the "secure" application itself.

Therefore, it is respectfully requested that the rejection of the claims be reconsidered and withdrawn.

Respectfully submitted,

Steven M. Hoffberg

By____________________
Steven M. Hoffberg
Reg. No. 33,511

MILDE & HOFFBERG, LLP
10 Bank Street-Suite 460
White Plains, NY 10606
(914) 949-3100